IAP-510+/512+

IEEE 802.11 a/n Access Point

User's Manual

Version 1.0

July, 2012

www.oring-networking.com

COPYRIGHT NOTICE

Copyright © 2011 ORing Industrial Networking Corp.
All rights reserved.
No part of this publication may be reproduced in any form without the prior written consent of ORing Industrial Networking Corp.

TRADEMARKS

is a registered trademark of ORing Industrial Networking Corp.
All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

WARRANTY

ORing warrants that all ORing products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). ORing will repair or replace products found by ORing to be defective within this warranty period, with shipment expenses apportioned by ORing and the distributor. This warranty does not cover product modifications or repairs done by persons other than ORing-approved personnel, and this warranty does not apply to ORing products that are misused, abused, improperly installed, or damaged by accidents.
Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

DISCLAIMER

Information in this publication is intended to be accurate. ORing shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ORing reserves the right to revise the contents of this publication without notice.

CONTACT INFORMATION

ORing Industrial Networking Corp.
3F., No.542-2, Zhongzheng Rd., Xindian Dist., New Taipei City 23148, Taiwan (R.O.C.)
Tel: +886-2-2218-1066 // Fax: +886-2-2218-1014
Website: www.oring-networking.com
Technical Support
E-mail: support@oring-networking.com
Sales Contact
E-mail: sales@oring-networking.com (Headquarters)
sales@oring-networking.com.cn (China)

Table of Content

Getting to Know Your Access Point 1

1.1 About the ORing Access Point 1

1.2 Software Features 1

1.3 Hardware Features 1

Hardware Installation 2

2.1 Pole Mounting Installation 2

2.2 Wall Mounting Installation 2

Hardware Overview 3

3.1 Front Panel 3

3.2 Front Panel LEDs 4

Cables and Antenna 4

4.1 Ethernet Cables 4

4.2 100Base-T(X)/10Base-T Pin Assignments 5

4.3 Wireless Antenna 6

Management Interface 7

5.1 Explore IAP-W510+ / W512+ 7

5.1.1 Open-Vision_Commander 7

5.2 Configuration by Web Browser 10

5.3 About Web-Based Management 10

5.4 Main Interface 11

5.5.1 Basic Setting 11

Setting Operation Mode 11

Setting WDS (Bridge Mode) 12

Setting Wireless 17
Client Setting 22
LAN Setting 23
Setting DHCP Server 25
5.5.2 Advanced Setting 26
Wireless 26
X-Roaming 29
MAC Filter 29
System Event 31
Email Settings 31
SNMP Settings 32
Syslog Server Settings 33
5.5.3 System Tools 33
Administrator 33
Date & Time 35
Configuration 37
Firmware Upgrade 38
Miscellaneous 38
5.5.4 System Status 39
System Info 39
System Log 40
Traffic Statistics 40
Wireless Clients 41
5.5.5 Online Help 41

Technical Specifications 42

Getting to Know Your Access Point

1.1 About the ORing Access Point

IAP-W510+ / W512+ are reliable IEEE802.11a/n WLAN Access Point with 1 Ethernet LAN port. It can be configured to operate in AP / Bridge / Repeater / AP-Client / Client mode. You can configure IAP-W510+ / W512+ by Window Utility or WEB interfaces via LAN port or WLAN interface. Therefore, IAP-W510+ / W512+ are one of the best communication solutions for wireless application.

1.2 Software Features

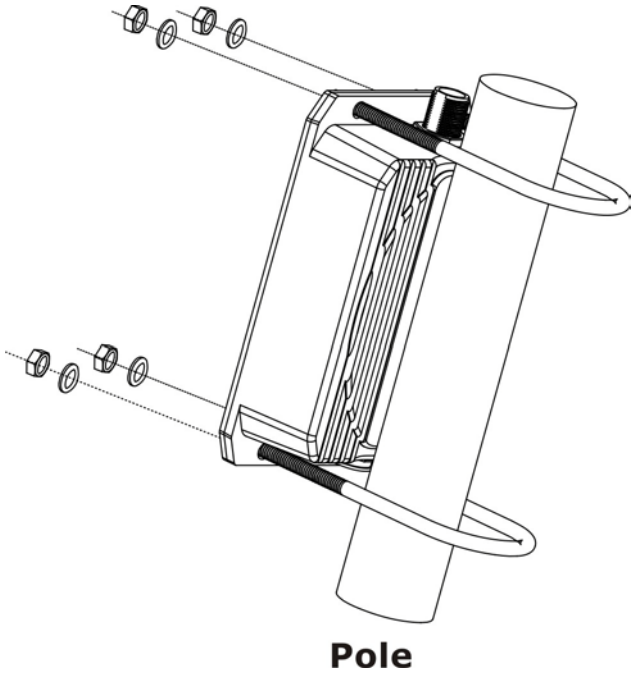
- High Speed Air Connectivity: WLAN interface support up to 300Mbps link speed connection
- Highly Security Capability: WEP/WPA/WPA2/WPA2-PSK/802.1x supported
- Support AP/Bridge/Repeater/AP-Client/Client Mode
- Secured Management by HTTPS
- Event Warning by Syslog, Email, SNMP Trap
- Support X-Roaming < 100 ms

1.3 Hardware Features

- Fully Compliant with IEEE802.3af
- 10/100Base-T(X) Ethernet port
- Casing: IP-67
- Dimensions(W x D x H) : 162 mm(W)x 102 mm(D)x 58 mm(H) for IAP-W510+;
  162 mm(W)x 102 mm(D)x 48 mm(H) for IAP-W512+
- Operating Temperature: -20 to 70°C
- Storage Temperature: -30 to 85°C
- Operating Humidity: 100% non-condensing

Hardware Installation

2.1 Pole Mounting Installation



2.2 Wall Mounting Installation

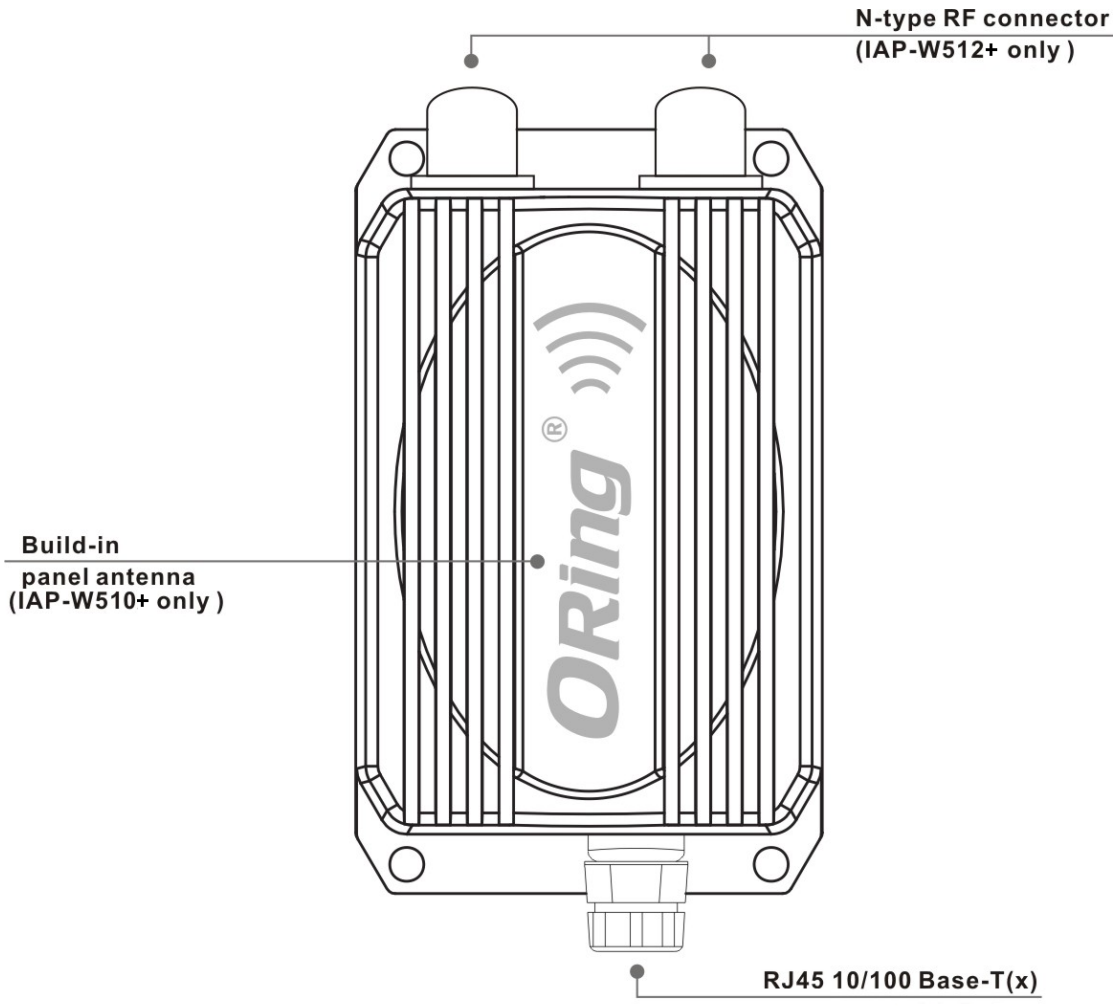
Hardware Overview

3.1 Front Panel

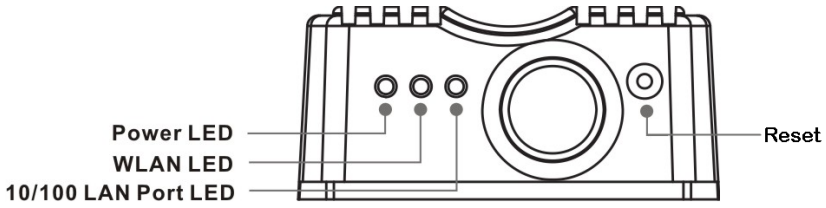
The following table describes the labels that stick on the IAP-W510+ / W512+.

Port	Description
10/100 RJ-45 fast Ethernet ports	10/100Base-T(X) RJ-45 fast Ethernet ports support auto-negotiation. Speed: auto
ANT.	2 x External N-type antenna connector for IAP-W512+, Build-in 15dBi panel antenna for IAP-W510+

IAP-W510+ IAP-W512+



3.2 Front Panel LEDs



LED	Color	Status	Description
Power LED	Green	Green On	Power activated
WLAN LED	Green	Green On	WLAN activated.
LAN Port LED	Green	Green On	Port link up
		Green blinking	Data transmitted.

Cables and Antenna

4.1 Ethernet Cables

The IAP-W510+ / W512+ WLAN AP have standard Ethernet ports. According to the link type, the AP use CAT 3, 4, 5,5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10Base-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100Base-T(X)	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45

4.2 100Base-T(X)/10Base-T Pin Assignments

With 100Base-T(X)/10Base-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

RJ-45 Pin Assignments

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	P.O.E. power input +
5	P.O.E. power input +
6	RD-
7	P.O.E. power input -
8	P.O.E. power input -

The IAP-510+ / 512+ AP support auto MDI/MDI-X operation. You can use a straight-through cable to connect PC and AP. The following table below shows the 10Base-T/ 100Base-T(X) MDI and MDI-X port pin outs.

MDI/MDI-X pins assignment

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	P.O.E. power input +	P.O.E. power input +
5	P.O.E. power input +	P.O.E. power input +
6	RD-(receive)	TD-(transmit)
7	P.O.E. power input -	P.O.E. power input -
8	P.O.E. power input -	P.O.E. power input -

Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.

4.3 Wireless Antenna

2 x External N-type antenna connector for IAP-W512+, Build-in 15dBi panel antenna for IAP-W510+

Management Interface

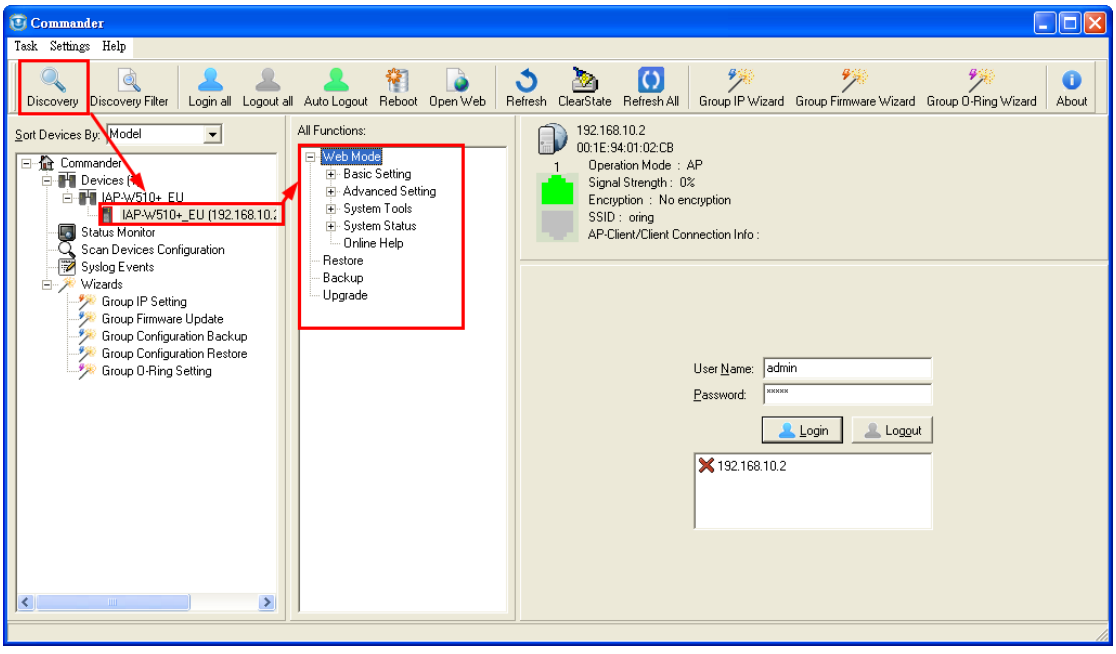
5.1 Explore IAP-W510+ / W512+

5.1.1 Open-Vision_Commander

Each model contains friendly software, Commander, to explore IAP-W510+ / W512+ on local area network.

Step 1: Open the Commander and click "Discover", the AP devices will show on the list.

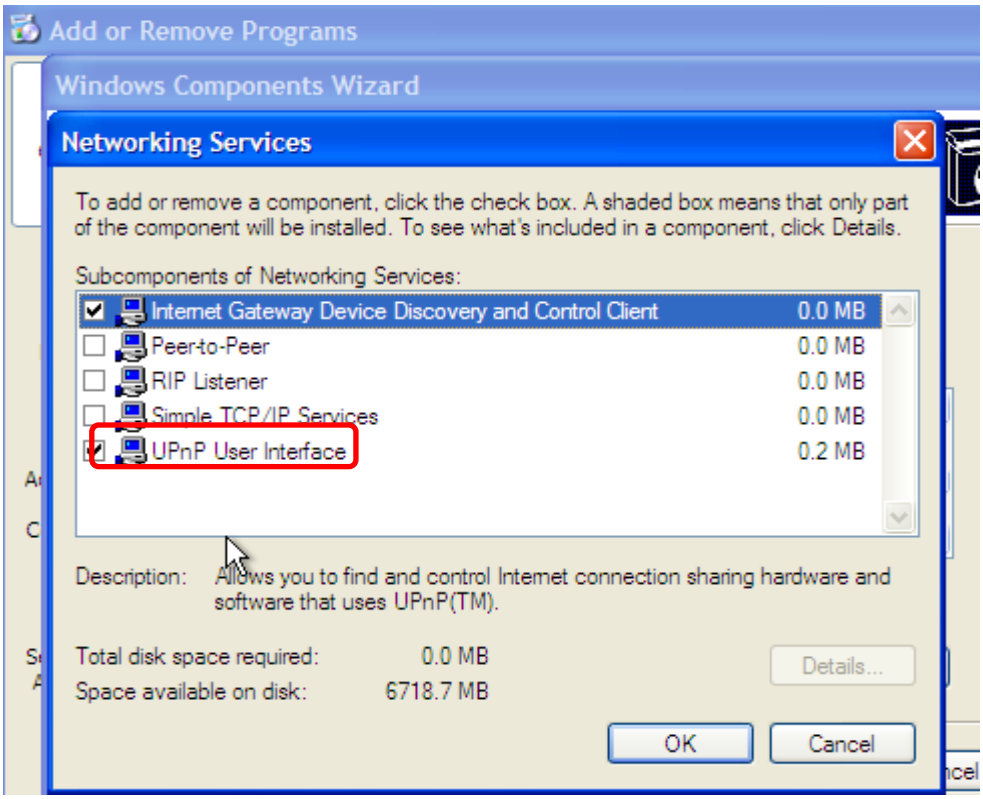
Step 2: Choose your access point, and it will show the AP function tree. Simultaneity, you can login and then set the AP.



User interface of Commander

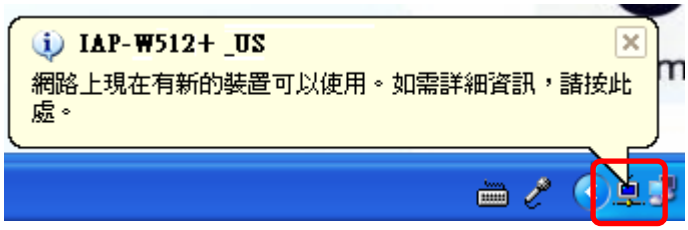
UPnP Equipment

Step 1: To check whether the UPnP UI of the computer is connected to the IAP-W510+ / W512+, go to **Control Panel > Add or Remove Programs > Windows Components Wizard > Networking Servers > UPnP User Interface** and pitch on the UPnP User Interface.


Add or Remove Programs
Windows Components Wizard
Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
Internet Gateway Device Discovery and Control Client 0.0 MB
Peer-to-Peer 0.0 MB
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
UPnP User Interface 0.2 MB
Description: Allows you to find and control Internet connection sharing hardware and software that uses UPnP(TM).
Total disk space required: 0.0 MB
Space available on disk: 6718.7 MB
Details...
OK
Cancel

UPnP configuration page

Step 2: At the right-below corner of the computer, you will find a sign of the UPnP equipment.



Step 3: Click the sign of the UPnP equipment, then you will find the UPnP equipment in the network neighborhood.

5.2 Configuration by Web Browser

This section introduces the configuration by Web browser.

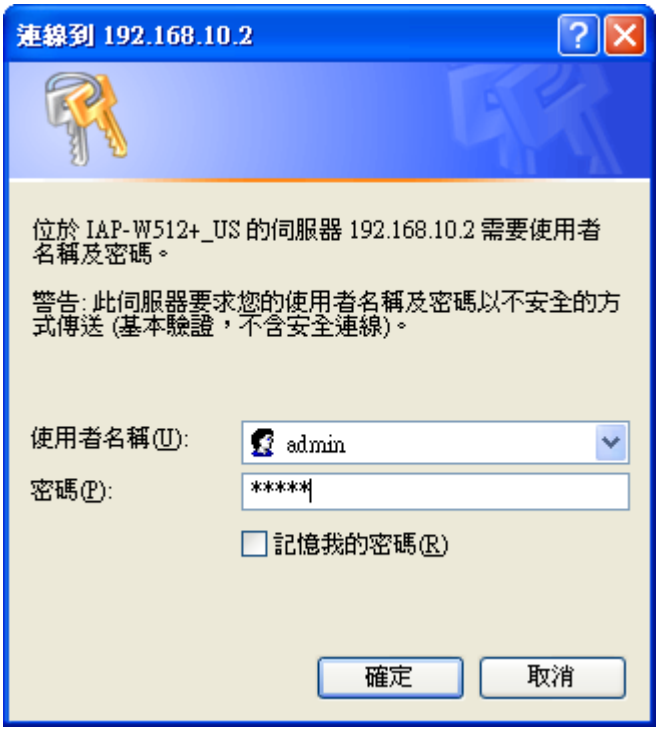
5.3 About Web-Based Management

An embedded HTML web site resides in flash memory in the system. It contains advanced management features and allows you to manage the AP from anywhere on the network through a standard web browser such as Microsoft Internet Explorer.

The Web-Based Management function supports Internet Explorer 5.0 or later. It is Based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

Note: By default, IE5.0 or later version does not allow Java Applets to open sockets. You need to explicitly modify the browser setting in order to enable Java Applets to use network ports.

Through the front section's information, you will see as following, enter your user name and your password, and then click **OK** to continue. If it is the first time to set up configuration, the default user name and password are "admin."

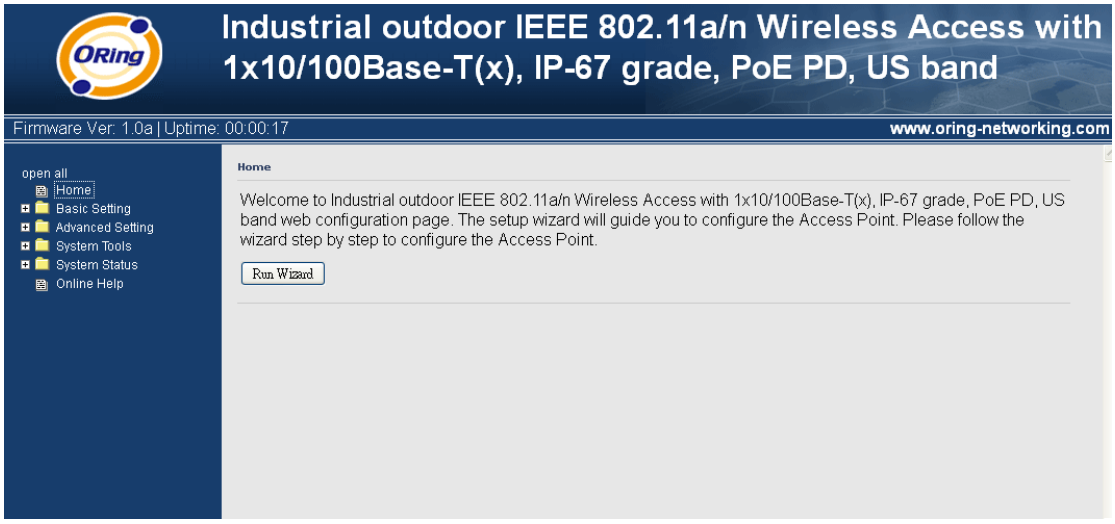


Login screen

Note: For security reasons, we strongly suggest you change the password. Click on **System Tools > Administrator** and modify the password.

5.4 Main Interface

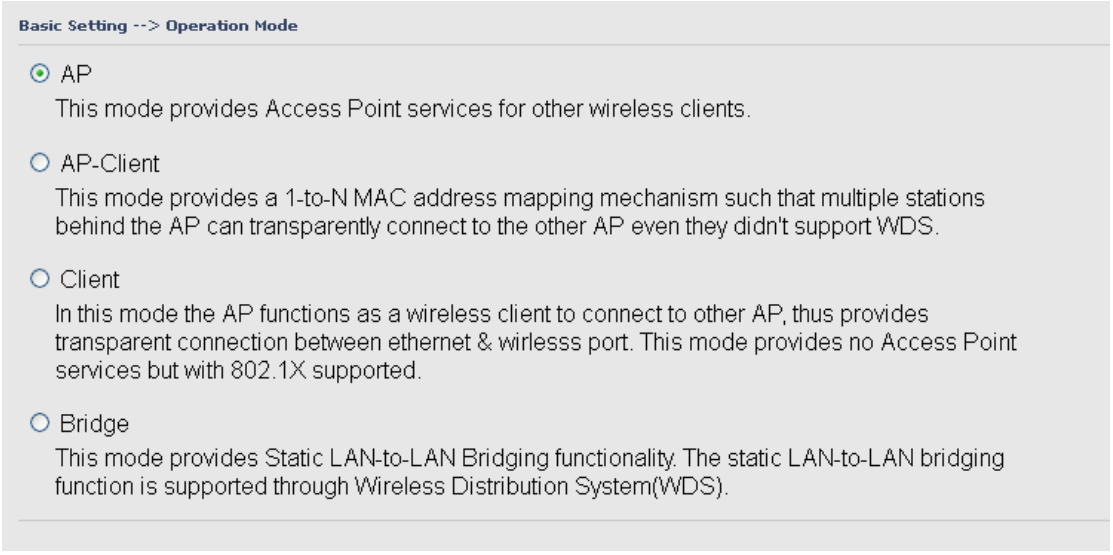
The **Home** screen will appear. Please click "Run Wizard" to go to the **Home > Setup Wizard** page to quick install the AP.


Industrial outdoor IEEE 802.11a/n Wireless Access with 1x10/100Base-T(x), IP-67 grade, PoE PD, US band
Firmware Ver: 1.0a | Uptime: 00:00:17
www.oring-networking.com
open all
Home
Basic Setting
Advanced Setting
System Tools
System Status
Online Help
Home
Welcome to Industrial outdoor IEEE 802.11a/n Wireless Access with 1x10/100Base-T(x), IP-67 grade, PoE PD, US band web configuration page. The setup wizard will guide you to configure the Access Point. Please follow the wizard step by step to configure the Access Point.
Run Wizard

Main interface

5.5.1 Basic Setting

Setting Operation Mode


Basic Setting --> Operation Mode
AP
This mode provides Access Point services for other wireless clients.
AP-Client
This mode provides a 1-to-N MAC address mapping mechanism such that multiple stations behind the AP can transparently connect to the other AP even they didn't support WDS.
Client
In this mode the AP functions as a wireless client to connect to other AP, thus provides transparent connection between ethernet & wirlesss port. This mode provides no Access Point services but with 802.1X supported.
Bridge
This mode provides Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System(WDS).

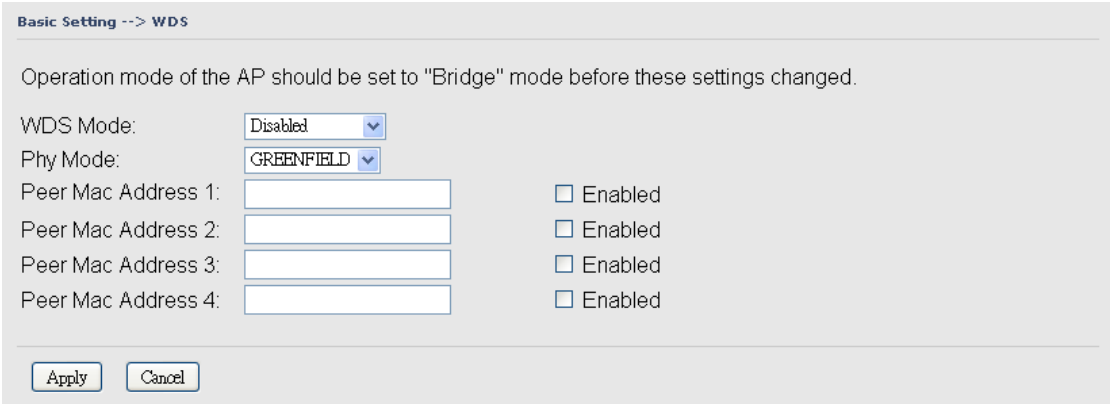
Operation mode interface

The following table describes the labels in this screen.

Label	Description
AP	This mode provides Access Point services for other wireless clients.
AP-Client	The AP-Client function provides a 1-to-N MAC address mapping mechanism such that multiple stations behind the AP can transparently connect to the other AP even they didn't support WDS.
Client	In this mode the AP functions as a wireless client to connect to other AP, thus provides transparent connection between Ethernet & wireless port. This mode provides no Access Point services but with 802.1X supported.
Bridge	This mode provides Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).

In each mode, the IAP-W510+ / W512+ forwards packet between its Ethernet interface and wireless interface for wired hosts on the Ethernet side, and wireless hosts on the wireless side.

Setting WDS (Bridge Mode)

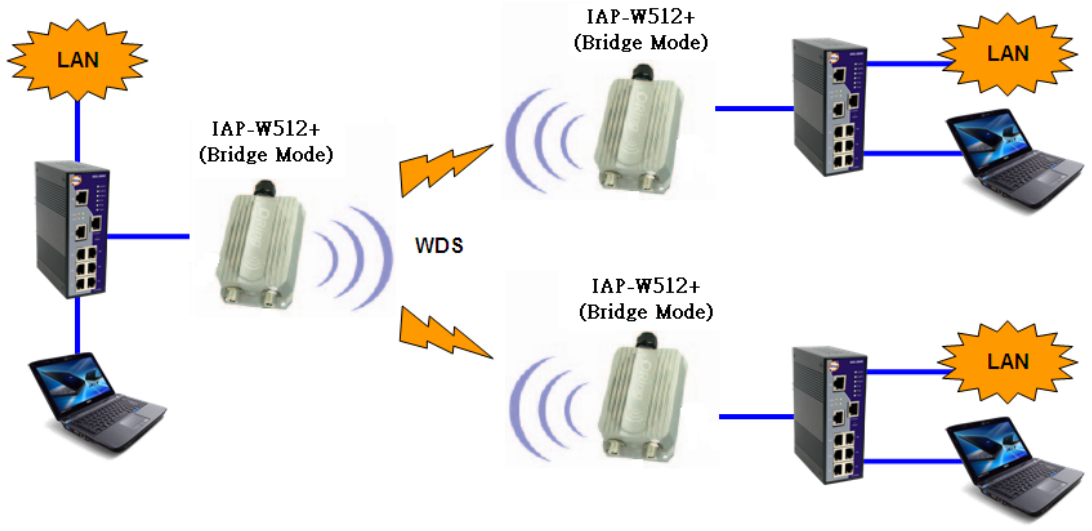


WDS setting interface

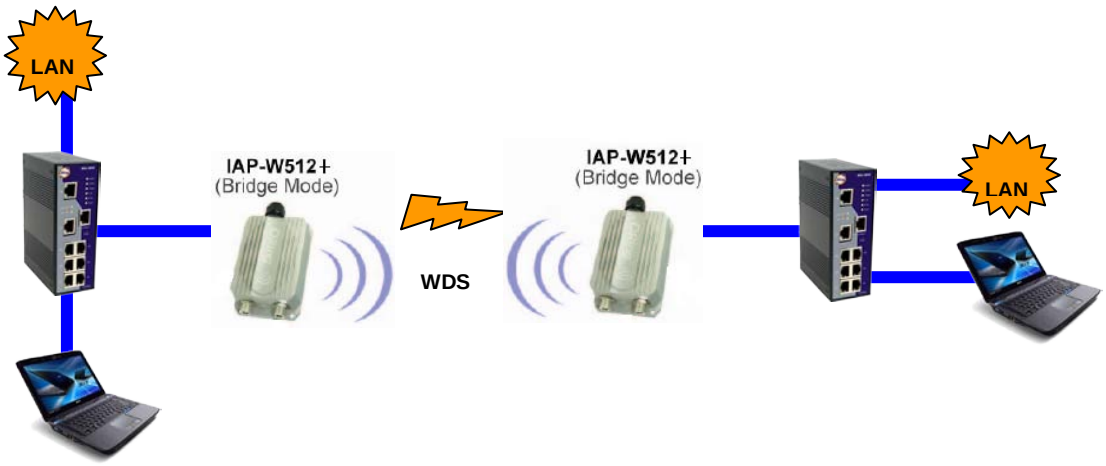
The following table describes the labels in this screen.

Label	Description
WDS Mode	This mode provides Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).
Phy Mode	It provides 3 options OFDM(11a mode) ,HTMIX(11 a/n mix mode) and GREENFIELD(11n mode)
Peer MAC Address	Set the Mac address(es) of other access point(s). Simultaneity, choose on "Enable".

This type of wireless link is established between two IEEE 802.11 access points. Wireless packets transmitted along the WDS link comply with the IEEE 802.11 WDS (Wireless Distribution System) format at the link layer.



Point-to-Multipoint WDS Link

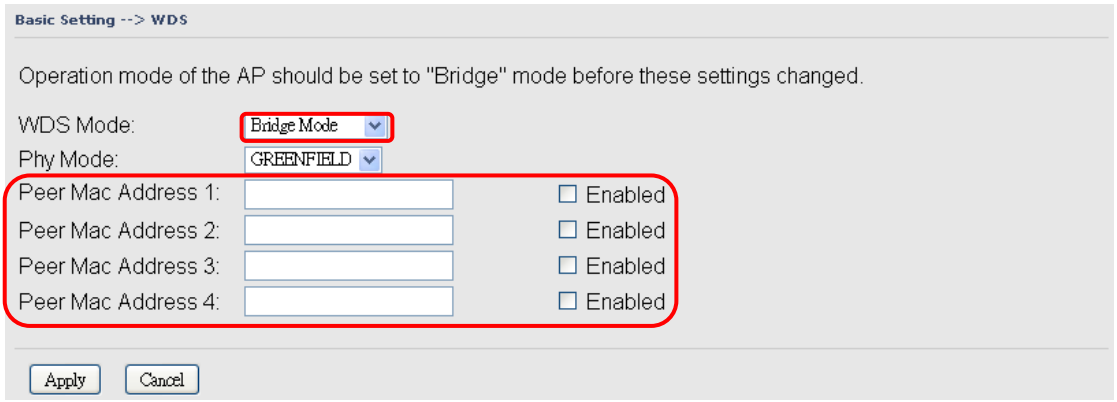


Point-to-Point WDS Link

First of all, if APs link with WDS mode, it should obey the following rules:

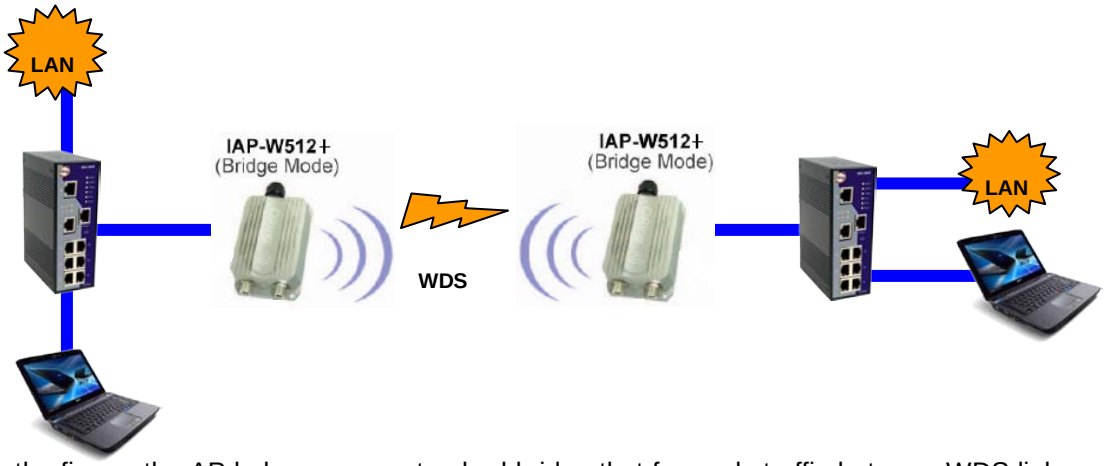
1. LAN IP Address should set different IP in the same network.
2. All AP's DHCP Server should set shutdown.
3. WDS should set Enable.
4. Each AP should have the same setting except 'Peer Mac Address' set to the other's Mac address
5. WEP Key and Channel should be the same, and each AP's SSID should be broadcast to see in the other's computer.
6. AP's distance should limit to a certainty area.

WDS –Bridge Mode



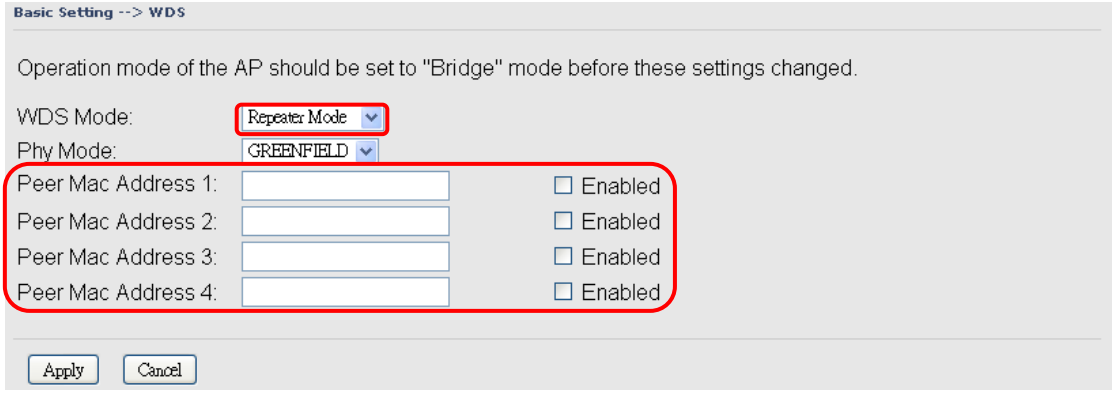
The peer WDS APs are according to the MAC address listed in "Peer Mac Address" fields.

The working principle of **Bridge Mode** as following:



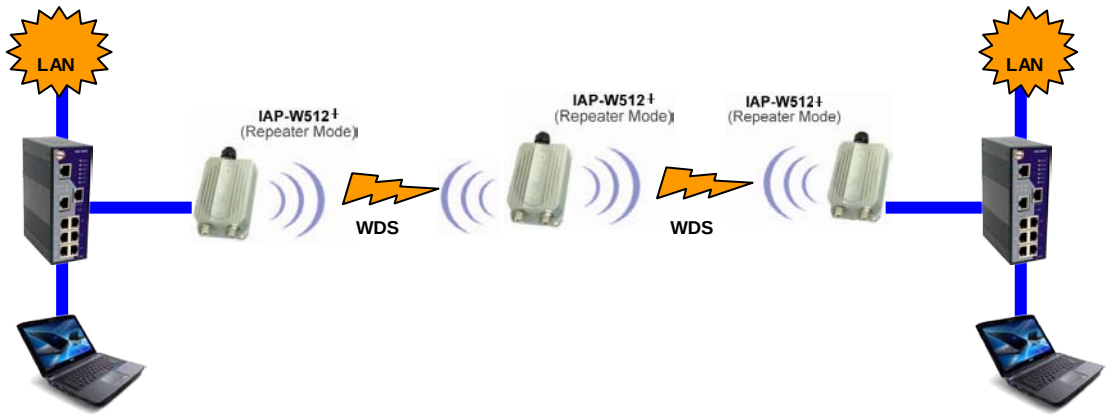
In the figure, the AP behaves as a standard bridge that forwards traffic between WDS links (links that connect to other AP/wireless bridges) and an Ethernet port. As a standard bridge, the AP learns MAC addresses of up to 64 wireless or 128 total wired and wireless network devices, which are connected to their respective Ethernet ports to limit the amount of data to be forwarded. Only data destined for stations which are known to reside on the peer Ethernet link, multicast data or data with unknown destinations need to be forwarded to the peer AP via the WDS link.

WDS –Repeater Mode



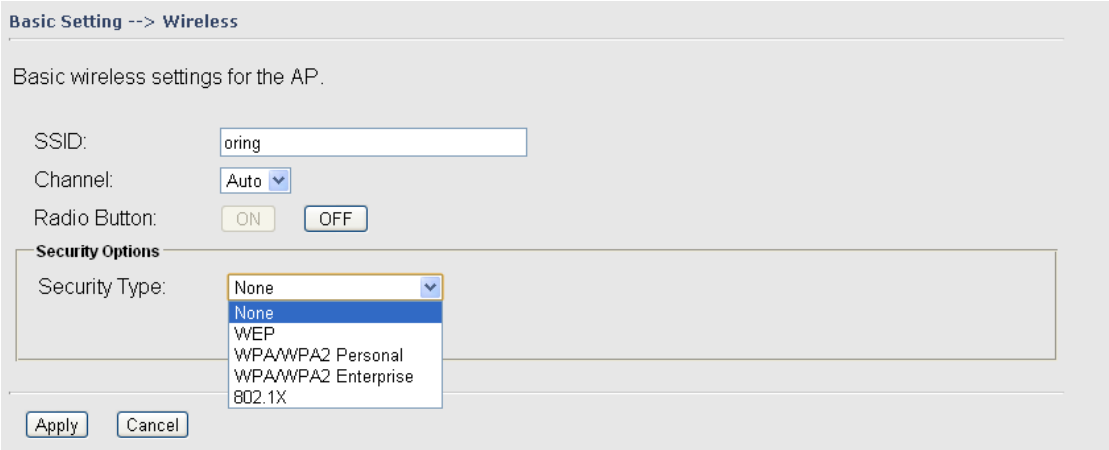
The peer WDS APs are according to the MAC address listed in "Peer Mac Address" fields.

The working principle of **Repeater Mode** as follows:



In the figure, Repeater is used to extend the range of the wireless infrastructure by forwarding traffic between associated wireless stations and another repeater or AP connected to the wired LAN.

Setting Wireless



The following table describes the labels in this screen.

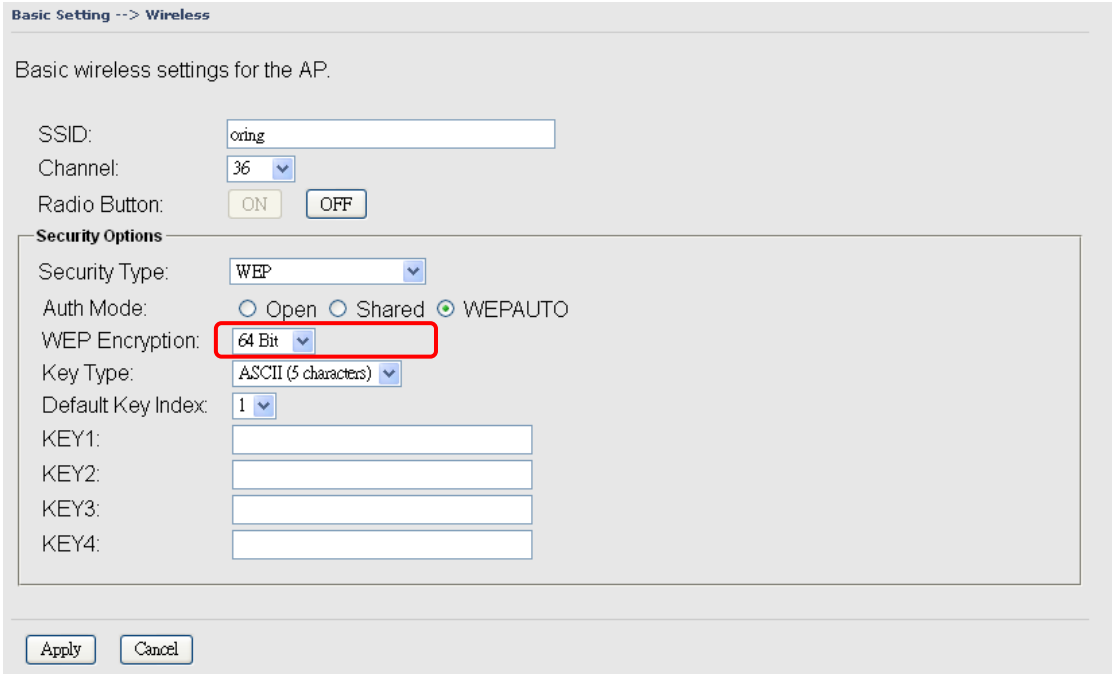
Label	Description
SSID	Service Set Identifier Default is the default setting. The SSID is a unique name that identifies a network. All devices on the network must share the same SSID name in order to communicate on the network. If you change the SSID from the default setting, input your new SSID name in this field.
Channel	Channel Auto is the default channel, input a new number if you want to change the default setting. All devices on the network must be set to the same channel to communicate on the network.
Security options	Select the type of security for your wireless network at **Security Type:** **None:** Select for no security. **WEP:** Select for security WEP. **WPA/WPA2 Personal:** Select for security WPA-PSK or WPA2-PSK without a RADIUS server.

	WPA/WPA2 Enterprise: Select for WPA or WPA2 (Wi-Fi Protected Access) authentication in conjunction with a RADIUS server. **802.1x:** Authentication through RADIUS server

Security Type – None

No security protection on your wireless LAN access.

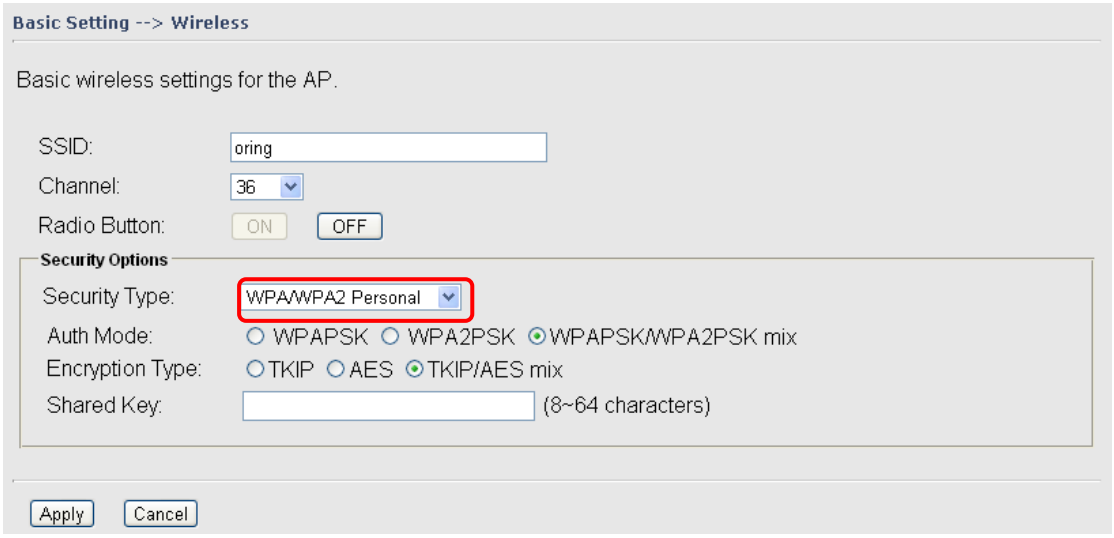
Security Type – WEP



1. Security Type: Select **WEP**
2. WEP Encryption: Select 64 Bit or 128 Bit WEP encryption.
3. Key Type: Select ASCII or Hex key type.
4. Default Key Index: Select one of the keys to be the active key.
5. Key 1-4: Input up to four encryption keys.

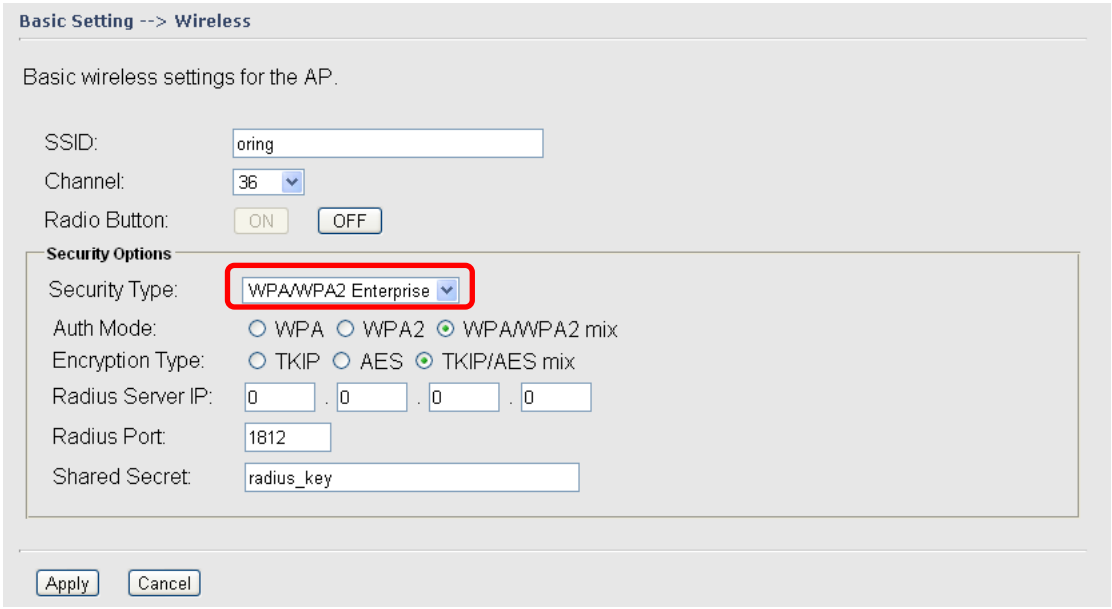
ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127. **Hex** digits consist of the numbers 0-9 and the letters A-F.

Security Type – WPA/WPA2 Personal



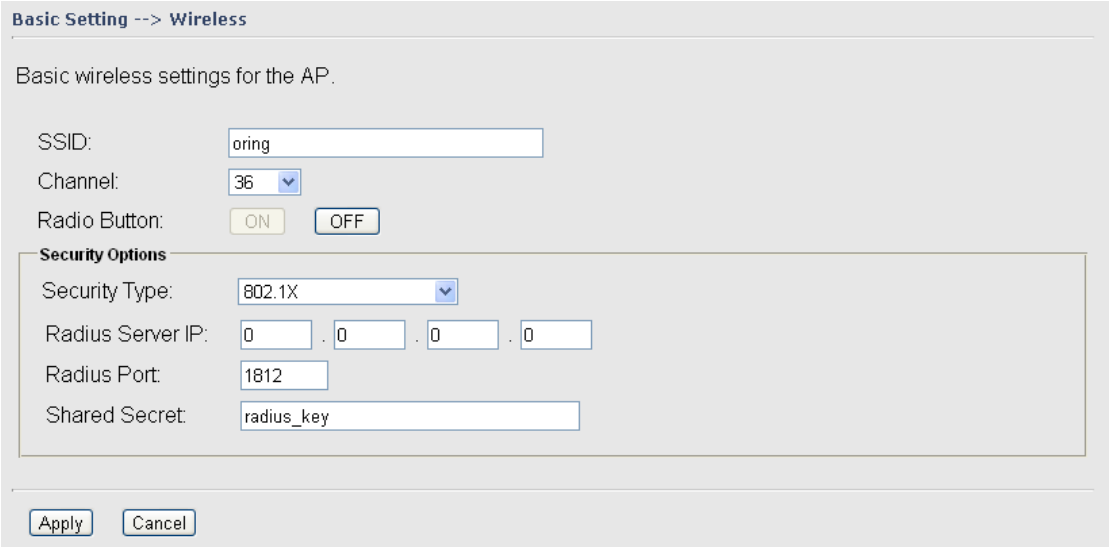
1. Security Type: Select **WPA-PSK/WPA2-PSK**.
2. Encryption Type: Select **TKIP** or **AES** encryption.
3. Share Key: Enter your password. The password can be between 8 and 64 characters.

Security Type – WPA /WPA2



1. Security Type: Select **WPA/WPA2**
2. Radius Server IP: Enter the IP address of the RADIUS Server.
3. Port: Enter the RADIUS port (1812 is default).
4. Shared Secret: Enter the RADIUS password or key.

Security Type – 802.1x

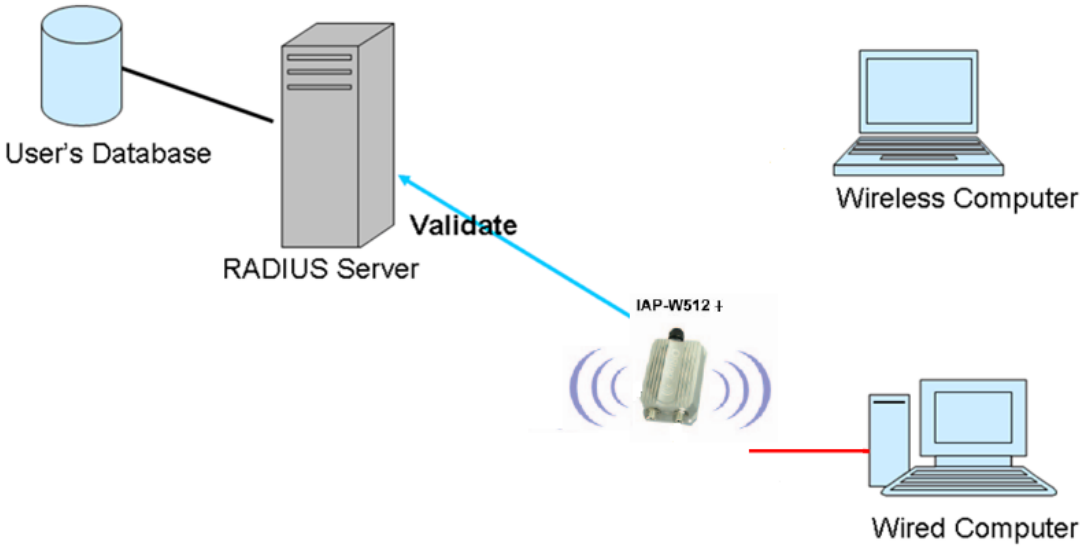


1. Security Type: Select **802.1x**
2. Radius Server IP: Enter the IP address of the RADIUS Server.
3. Port: Enter the RADIUS port (1812 is default).
4. Shared Secret: Enter the RADIUS password or key.

RADIUS (Remote Authentication Dial-in User Service) is the industrial standard agreement, and it is used to provide an identify verification. The Radius customer (is usually a dial-in server, VPN server or wireless point) send your proof and the conjunction parameter to the Radius server by Radius news. The Radius server validates the request of the Radius customer, and return Radius news to back.

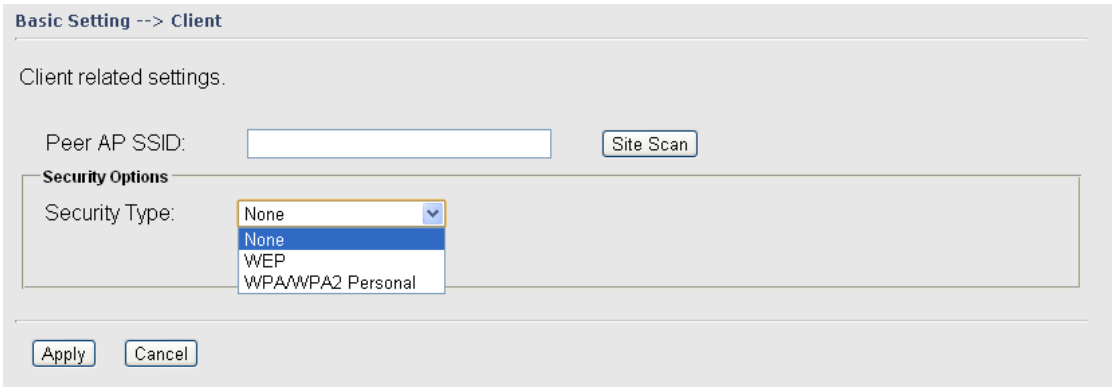
Radius server validates your proof, also carry on the authorization. So the Radius server received by ISA server responded (point out the customer carries proof to be not granted) and it means that the Radius server did not authorize you to carry. Even if the proof has already passed an identity verification, the ISA server may also refuse you to carry a claim according to the authorization strategy of the Radius server.

The principle of the Radius server shows in the following pictures:

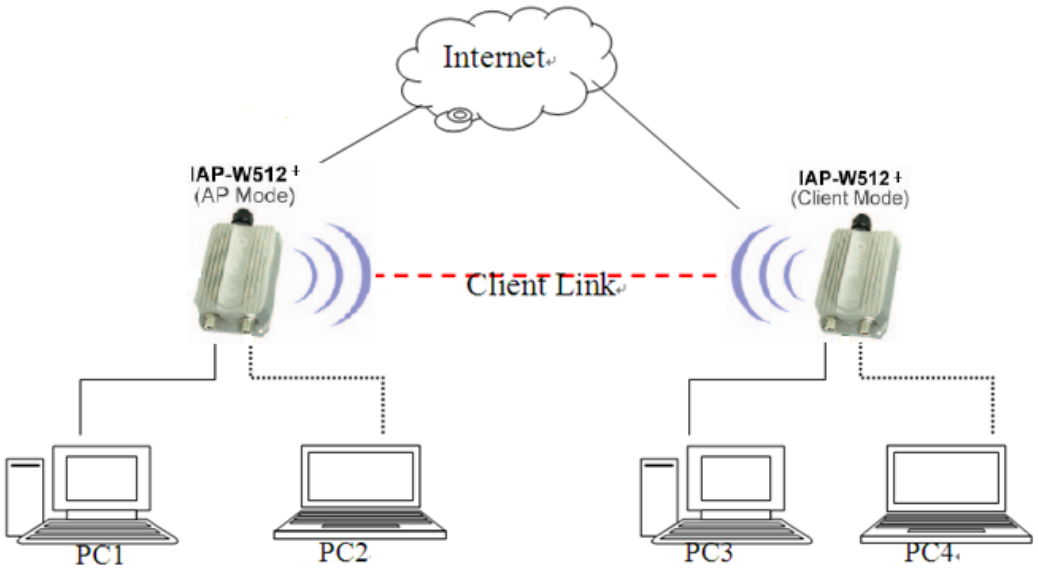


Client Setting

The **Basic setting—>Client Setting** page is mainly set the client which through the SSID and Security to connect to other AP. In this mode, the Security Type should be the same with the AP Server.



The principle of the AP-Client/Client mode shows in the following pictures:



Result:

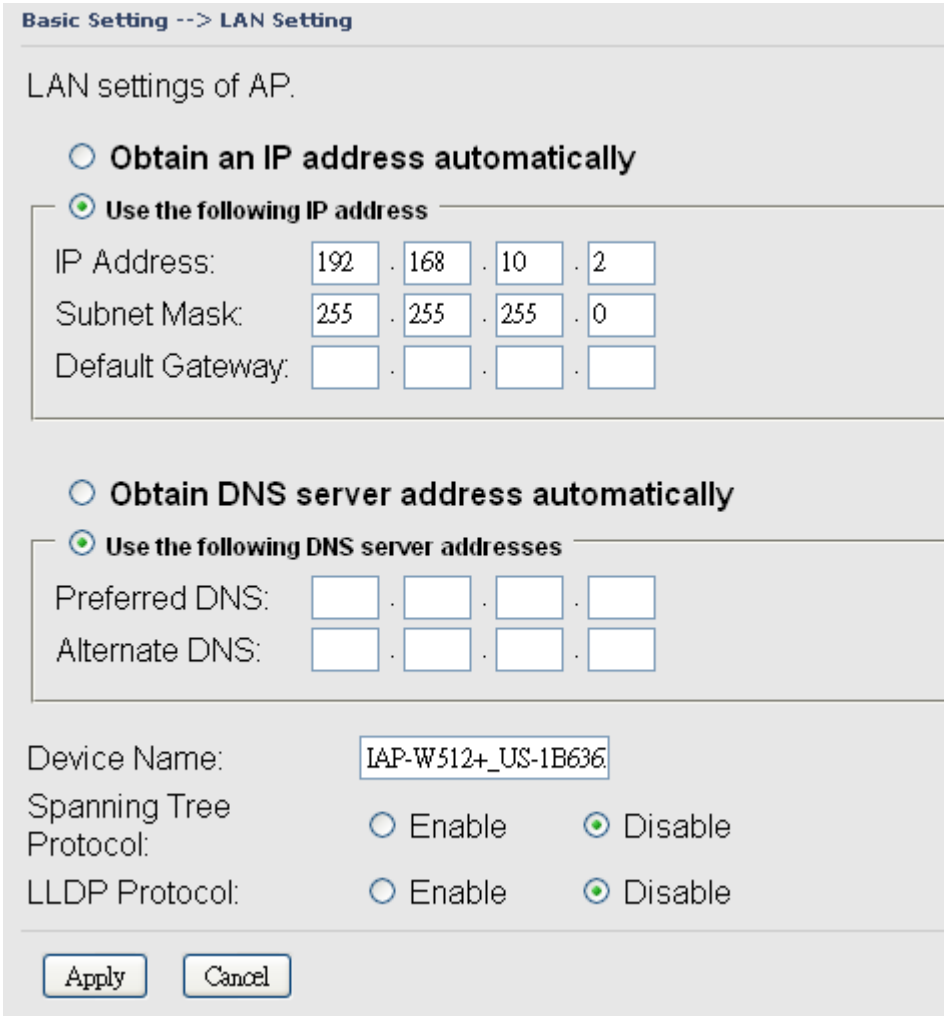
1. PC1, PC2 can visit PC3, PC4 and AP Client
2. PC3, PC4 can visit PC1, PC2 and AP
3. AP Client can visit AP

The following table describes the labels in this screen.

Label	Description
Peer AP SSID	Enter the other AP which used for AP mode.
Site Scan	You can scan the APs which used for AP mode in the certainty area
Security Type	Set the same security with the AP which you want to connect.

LAN Setting

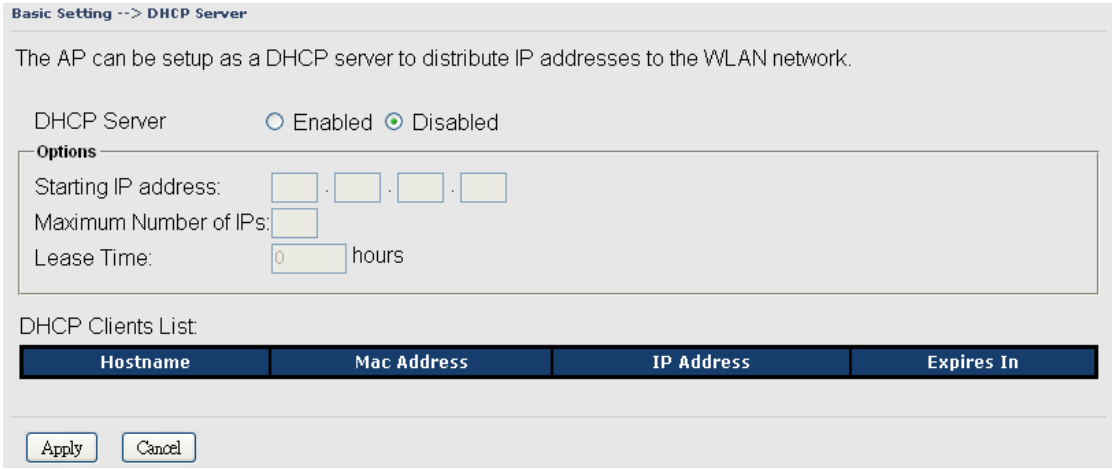
The **Basic Setting > LAN Setting** page is mainly set IP address for LAN interface. To access the AP normally, a valid IP address of your LAN should be specified to the LAN interface. The default IP setting is DHCP server (Obtain an IP address automatically).


Basic Setting --> LAN Setting
LAN settings of AP.
Obtain an IP address automatically
Use the following IP address
IP Address: 192 . 168 . 10 . 2
Subnet Mask: 255 . 255 . 255 . 0
Default Gateway:
Obtain DNS server address automatically
Use the following DNS server addresses
Preferred DNS:
Alternate DNS:
Device Name: IAP-W512+_US-1B636
Spanning Tree Protocol: Enable Disable
LLDP Protocol: Enable Disable
Apply
Cancel

The following table describes the labels in this screen.

Label	Description
Obtain an IP address automatically	Select this option if you would like to have an IP address automatically assigned to the IAP-W510+ / W512+ by DHCP server in your network
Use the following IP address	Select this option if you are manually assigning an IP address. **IP Address:** There is a default IP address in the AP, and you can input a new IP address. **Subnet Mask:** 255.255.255.0 is the default Subnet Mask. All devices on the network must have the same subnet mask to communicate on the network. **Default Gateway:** Enter the IP address of the router in your network.
Obtain DNS server address automatically	This option is selected by DHCP server.
Use the following DNS server addresses	This option is selected by manually set **Preferred DNS:** There is a default DNS server, and you can input another new DNS server. **Alternate DNS:** There is a default DNS server, and you can input another new DNS server.

Setting DHCP Server

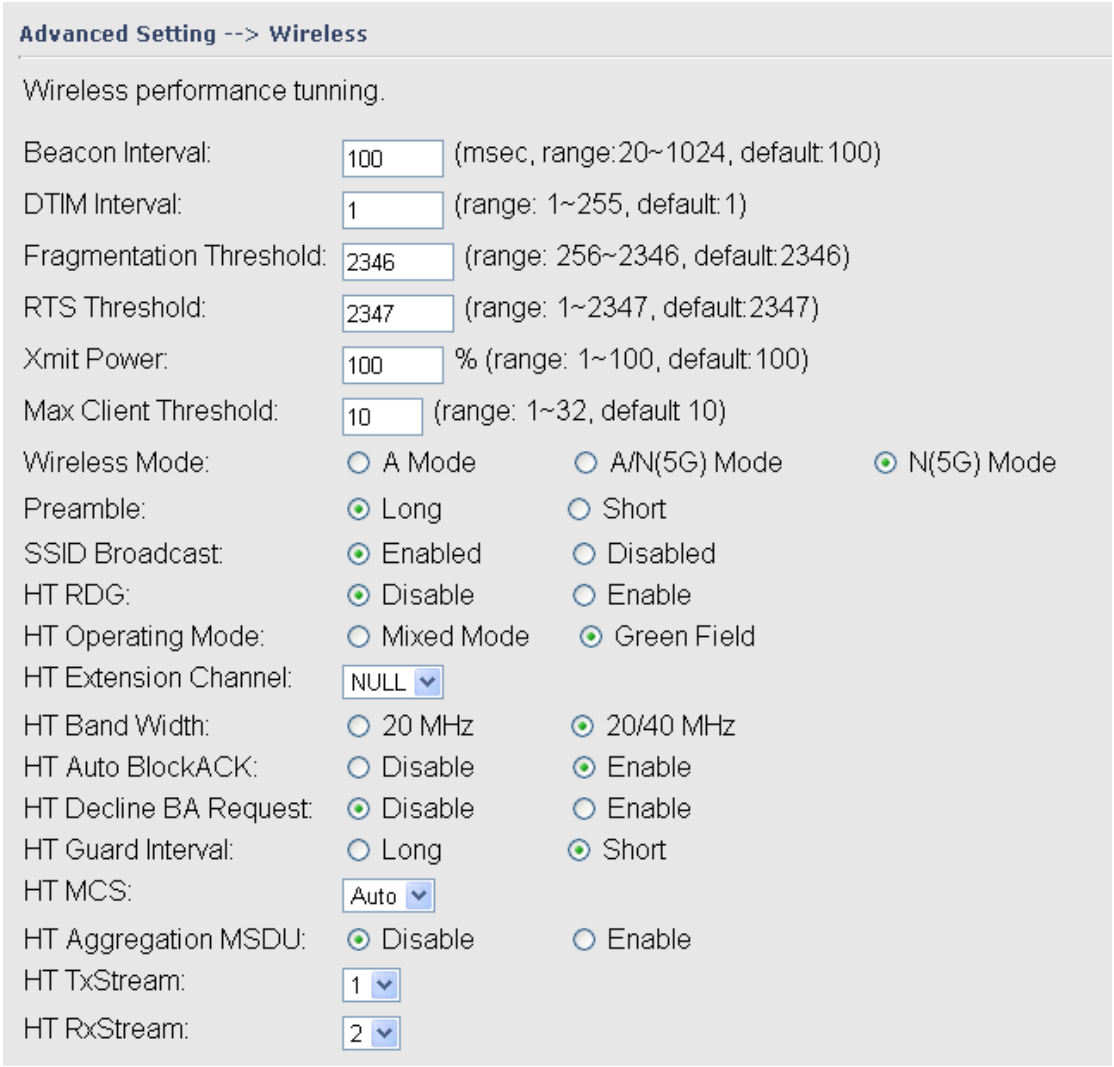


The following table describes the labels in this screen.

Label	Description
DHCP Server	Enable or Disable the DHCP Server function. Enable – the AP will be the DHCP server on your local network
Start IP Address	The dynamic IP assign range. Low IP address is the beginning of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. 192.168.1.100 will be the Start IP address.
Maximum Number of IPs	The dynamic IP assign range. High IP address is the end of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. **100** will be enter into textbox.
Lease Time (Hour)	It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn't know that the dynamic IP is idle.
DHCP Clients List	List the devices on your network that are receiving dynamic IP addresses from the IAP-W510 / 512.

5.5.2 Advanced Setting

Wireless


Advanced Setting --> Wireless
Wireless performance tunning.
Beacon Interval: 100 (msec, range:20~1024, default:100)
DTIM Interval: 1 (range: 1~255, default:1)
Fragmentation Threshold: 2346 (range: 256~2346, default:2346)
RTS Threshold: 2347 (range: 1~2347, default:2347)
Xmit Power: 100 % (range: 1~100, default:100)
Max Client Threshold: 10 (range: 1~32, default 10)
Wireless Mode: A Mode A/N(5G) Mode N(5G) Mode
Preamble: Long Short
SSID Broadcast: Enabled Disabled
HT RDG: Disable Enable
HT Operating Mode: Mixed Mode Green Field
HT Extension Channel: NULL
HT Band Width: 20 MHz 20/40 MHz
HT Auto BlockACK: Disable Enable
HT Decline BA Request: Disable Enable
HT Guard Interval: Long Short
HT MCS: Auto
HT Aggregation MSDU: Disable Enable
HT TxStream: 1
HT RxStream: 2

The following table describes the labels in this screen.

Label	Description
Beacon Interval	The default value is 100. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the AP to synchronize the wireless network. 50 is recommended in poor reception.
DTIM Interval	The default value is 1. This value, between 1 and 255 milliseconds, indicates the interval of the Delivery Traffic Indication

	Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.
Fragmentation Threshold	This value should remain at its default setting of 2346. The range is 256-2346 bytes. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended.
RTS Threshold	This value should remain at its default setting of 2347. The range is 0-2347 bytes. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The AP sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.
Xmit Power	Control RF transmission power, this value ranges from 1 - 100 percent, default value is 100 percent.
Wireless Network Mode	If you have 802.11N (5G) devices in your network, then keep the default setting, N (5G) mode. If you have only Wireless-A

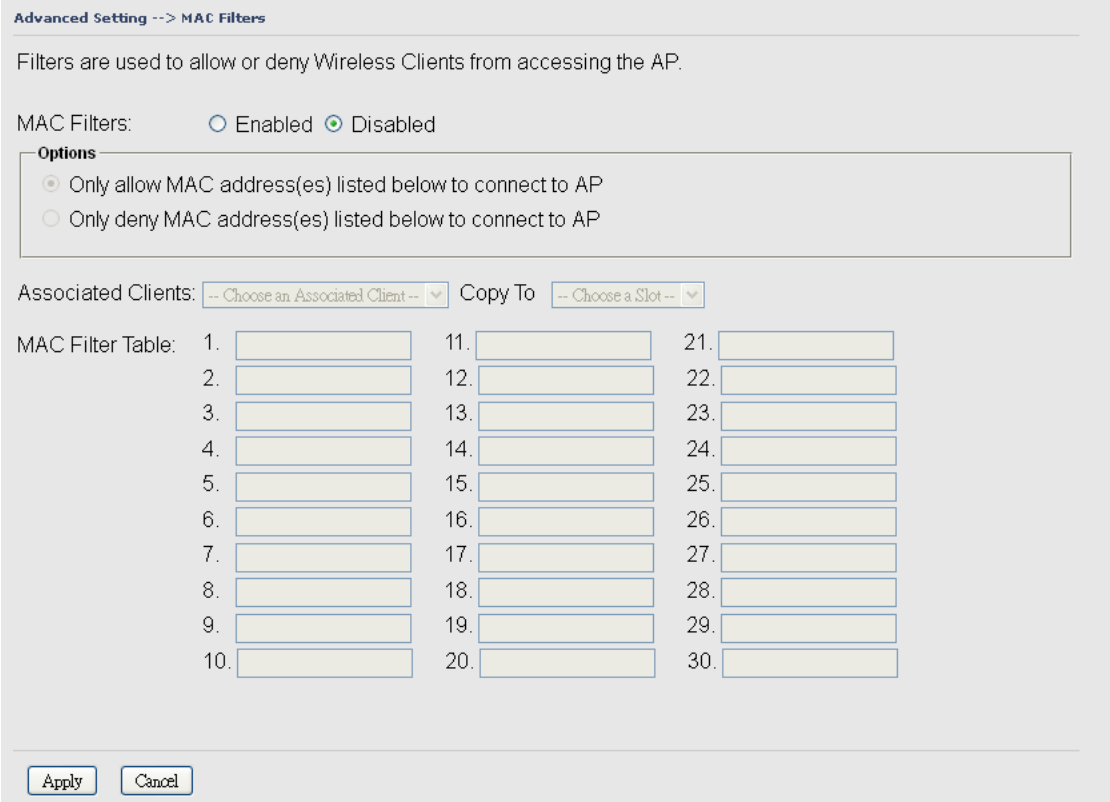
	devices, select A Mode or A/N mix mode.
Transmission Rate	The default setting is **Auto**. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or keep the default setting, Auto, to have the AP automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the AP and a wireless client.
Preamble	Values are Long and Short, default value is Long. If your wireless device supports the short preamble and you are having trouble getting it to communicate with other 802.11b devices, make sure that it is set to use the long preamble
SSID Broadcast	When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the AP. To broadcast the AP SSID, keep the default setting, Enable. If you do not want to broadcast the AP SSID, then select Disable.
Max Client Threshold	Max number of client equipment setting. When client number over this value AP will reject roaming equipment connection.(This value just effect on AP-mode equipment)

X-Roaming

X-Roaming	**Disable:** Disable X-Roaming protocol. **Standard:** Roaming group does not require the same wireless channel, but slower to switch than the "fixed channel" mode **Fixed channel:** Roaming group must be required the same wireless channel, but faster to switch than the "Standard" mode
Roaming Signal Threshold	Roaming signal threshold setting. When signal below this value AP will roaming to another client target which the same SSID, security option and signal strongest within the environment.(This value just effect on client-mode equipment)

MAC Filter

Use **Advanced Setting > MAC Filters** to allow or deny wireless clients, by their MAC addresses, from accessing the IAP-W510+ / W512+. You can manually add a MAC address or select the MAC address from **Connected Clients** that are currently connected to the AP.

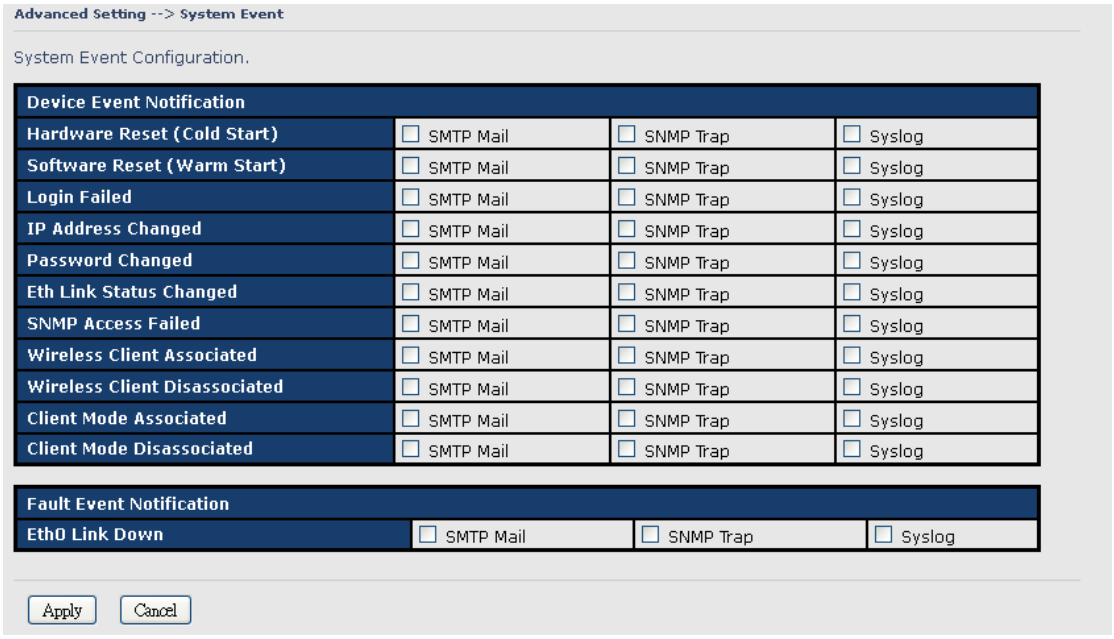

Advanced Setting --> MAC Filters
Filters are used to allow or deny Wireless Clients from accessing the AP.
MAC Filters: Enabled Disabled
Options
Only allow MAC address(es) listed below to connect to AP
Only deny MAC address(es) listed below to connect to AP
Associated Clients: -- Choose an Associated Client --
Copy To -- Choose a Slot --
MAC Filter Table:
1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
11. 12. 13. 14. 15. 16. 17. 18. 19. 20.
21. 22. 23. 24. 25. 26. 27. 28. 29. 30.
Apply
Cancel

The following table describes the labels in this screen.

Label	Description
MAC Filter	Enable or disable the function of MAC filter. MAC address allowed or denied option is selected by you.
MAC Filter List	This list will display the MAC addresses that are in the selected filter.
Connected Clients	This list will display the wireless MAC addresses that linked with AP.
MAC Address	MAC addresses need to be added to or clear from MAC filter list.
Apply	Click Apply to set the configurations.

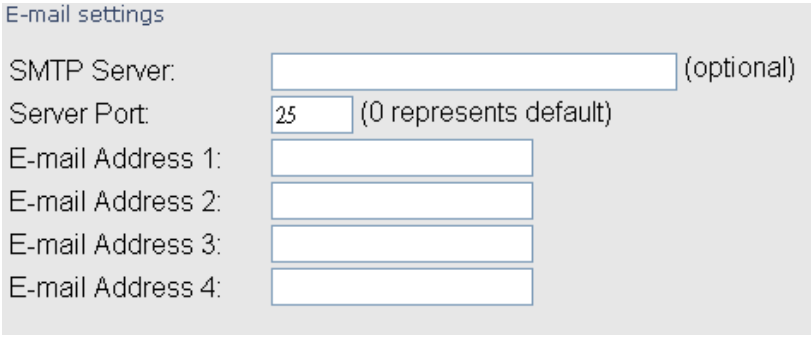
System Event

When the AP event triggered, the notification procedure will be performed according to the type of the event. Which notification would be performed depends on the selection of corresponding option in the **Advanced Setting > System Event** page.



System events record the activities of the AP system. When the setting changes or action performs, the event will be sent to administrator by email. A trap will also be sent to SNMP server. The Syslog will record the event locally and may send the log remotely to a Syslog server.

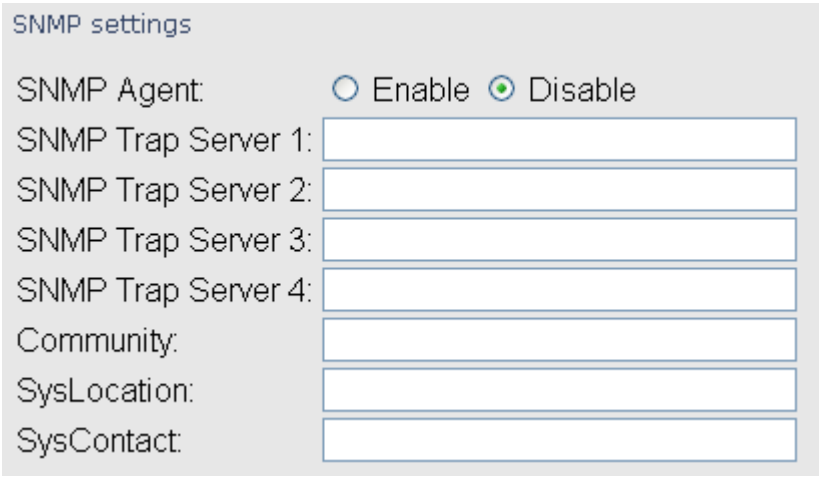
Email Settings



The following table describes the labels in this screen.

Label	Description
SMTP Server	Simple Message Transfer Protocol, enter the backup host to use if primary host is unavailable while sending mail by SMTP server.
Server Port	Specify the port where MTA can be contacted via SMTP server.
E-mail Address 1-4	Inputs specify the destination mail address.

SNMP Settings



The following table describes the labels in this screen.

Label	Description
SNMP Agent	SNMP (Simple Network Management Protocol) Agent is a service program that runs on the access point. The agent provides management information to the NMS by keeping track of various operational aspects of the AP system. Turn on to open this service and off to shutdown it.
SNMP Trap Server 1-4	Specify the IP of trap server, which is the address to which it will send traps AP generates.
Community	Community is essentially password to establish trust between managers and agents. Normally "public" is used for read-write

	community.
SysLocation	Specify sysLocation string.
SysContact	Specify sysContact string.

Syslog Server Settings

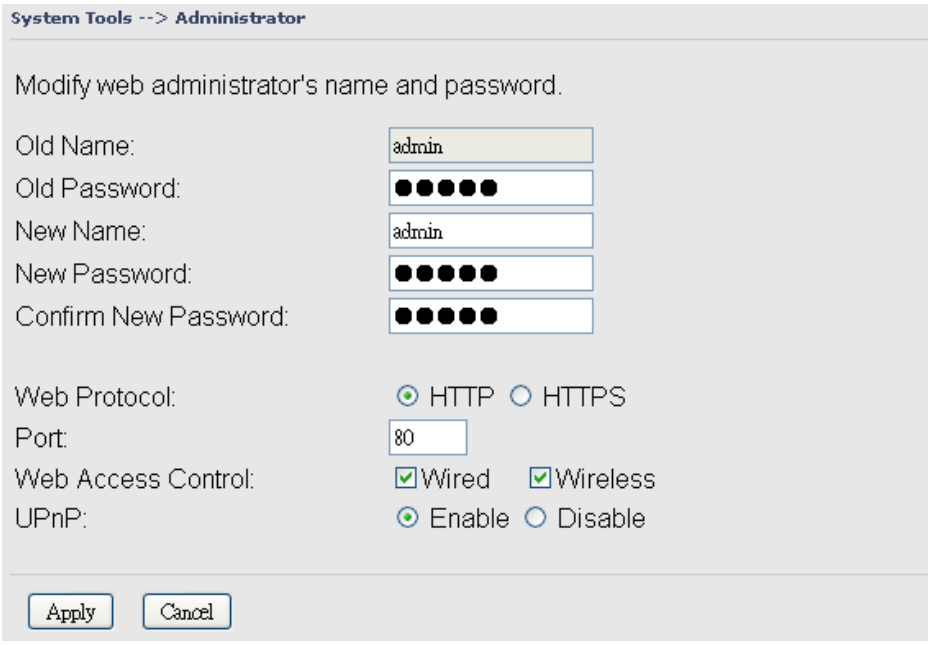
The following table describes the labels in this screen.

Label	Description
Syslog Server IP	Not only the syslog keeps the logs locally, it can also log to remote server. Specify the IP of remote server. Leave it blank to disable logging remotely.
Syslog Server Port	Specify the port of remote logging. Default port is 514.

5.5.3 System Tools

Administrator

In this page, you can change the username and password. The new password must be typed twice to confirm (the default Name and Password is "**admin**" and "").



The following table describes the labels in this screen.

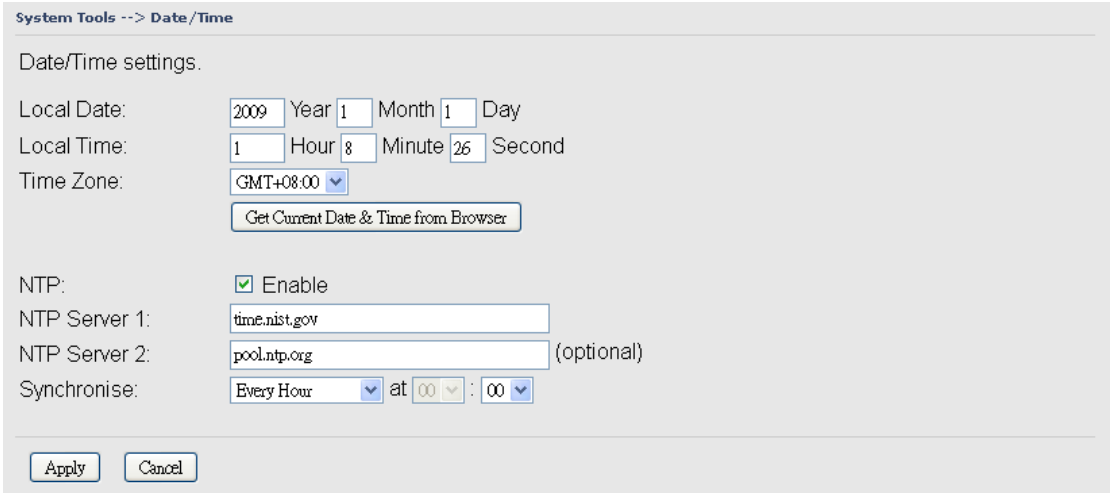
Label	Description
Old Name	This field displays the old login name. It's read only. The default value of login name is "admin".
Old Password	Before making a new setting, you should provide the old password for a verify check. Acceptable inputs of this field contains '0-9', 'a-z', 'A-Z' and must be between 0 to 15 characters in length. The factory default value of login password is null.
New Name	Enter a new login name. Acceptable inputs of this field contains '0-9', 'a-z', 'A-Z' and must be between 1 to 15 characters in length. This field can't accept null input.
New Password	Enter a new login password. Acceptable inputs of this field contains '0-9', 'a-z', 'A-Z' and must be between 0 to 15 characters in length.
Confirm New	Retype the password to confirm it. Acceptable inputs of this field

Password	contains '0-9', 'a-z', 'A-Z' and must be between 0 to 15 characters in length.
Web Protocol	Choose on the protocol for web. The default value is **HTTP**, if you want the web pages' security is better, choose the **HTTPS** protocol.
Port	Corresponding to the Web protocol, there is a default port (HTTP: 80, HTTPS: 443). And you can enter another number which should be in range of 1-65535.
Web Access Control	Choose the checkbox of the Wired and Wireless; you can visit the web page through the mode you choose.
UPnP	Pitch on "Enable", and the UPnP will display in the right-behind corner.

HTTPS (HTTP over SSL) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

Date & Time

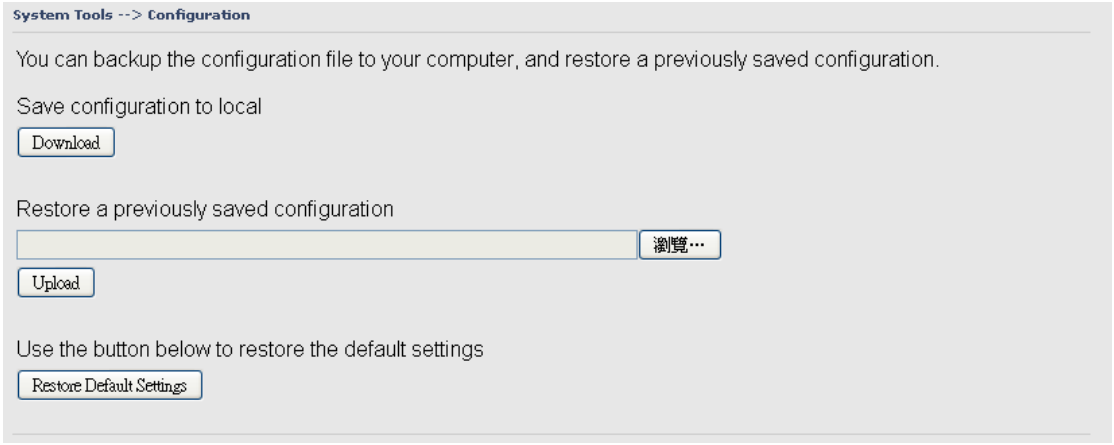
In this page, set the date & time of the device. The correct date & time will be helpful for logging of system events. A NTP (Network Time Protocol) client can be used to synchronize date & time with NTP server.



The following table describes the labels in this screen.

Label	Description
Local Date	Set local date manually.
Local Time	Set local time manually.
Time Zone	Select the time zone manually
Get Current Date & Time from Browser	Click this button, you can set the time from browser.
NTP	Enable or disable NTP function to get the time from the NTP server.
NTP Server 1	The initial choice about NTP Server.
NTP Server 2	The second choice about NTP Server.
Synchronize	Set the time, and the AP's time synchronize with the NTP Server at the time

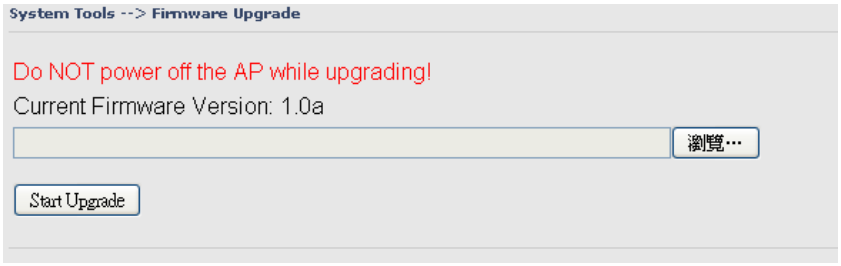
Configuration


System Tools --> Configuration
You can backup the configuration file to your computer, and restore a previously saved configuration.
Save configuration to local
Download
Restore a previously saved configuration
瀏覽...
Upload
Use the button below to restore the default settings
Restore Default Settings

The following table describes the labels in this screen.

Label	Description
Download configuration	The current system settings can be saved as a file onto the local hard drive.
Upload configuration	The saved file or any other saved setting file can be uploaded back on the AP. To reload a system settings file, click on **Browse** to browse the local hard drive and locate the system file to be used. Click **Upload** when you have selected the file to be loaded back onto the AP.
Restore Default Settings	You may also reset the IAP-510 / 512 back to factory settings by clicking on **Restore Default Settings**. Make sure to save the unit's settings before clicking on this button. You will lose your current settings when you click this button.

Firmware Upgrade

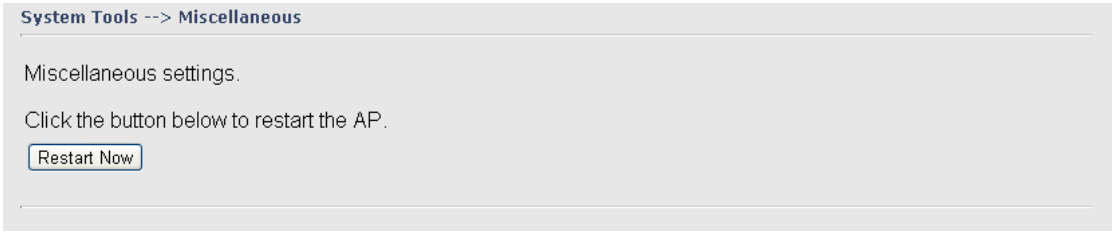


New firmware may provide better performance, bug fixes or more functions. To upgrade, you need a firmware file correspond to this AP model. It will take several minutes to upload and upgrade the firmware. After the upgrade is done successfully, the access point will reboot and get revalidated.

Notice: DO NOT POWER OFF THE AP OR PRESS THE RESET BUTTON WHILE THE FIRMWARE IS BEING UPGRADED.

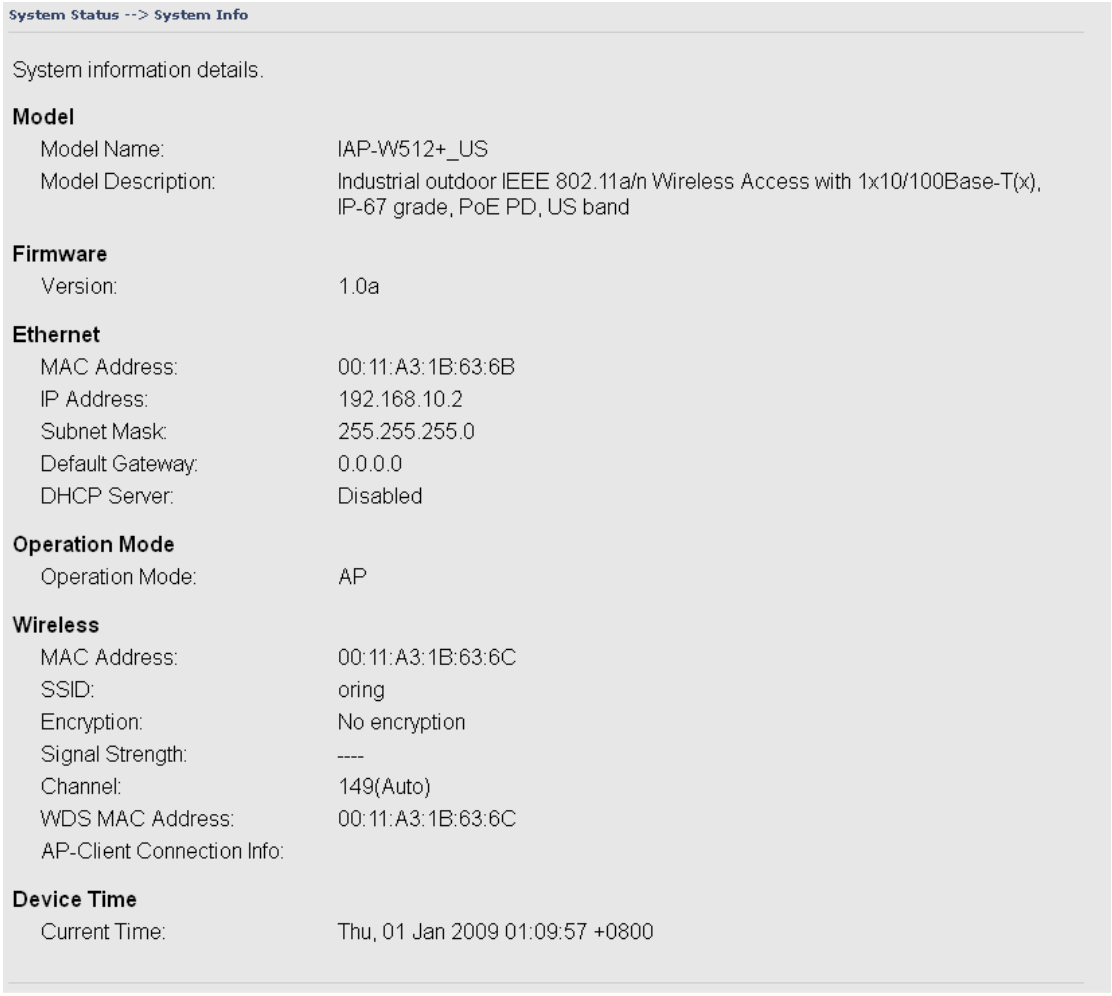
Miscellaneous

If you want to restart the access point through the **Warm Reset**, click **Restart Now** to restart the AP.



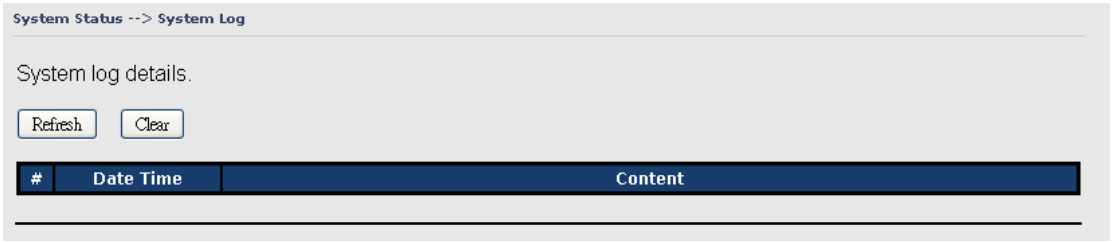
5.5.4 System Status

System Info



This page displays the current information for the IAP-W510+ / W512+. It will display model name, as well as firmware version, Ethernet, Wireless info and device time.

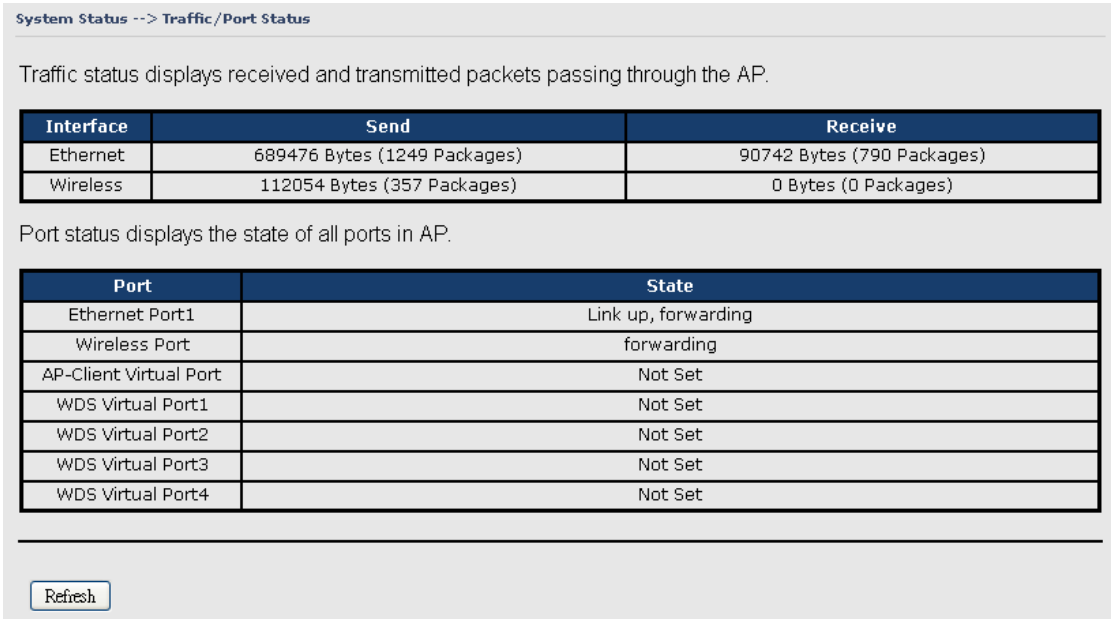
System Log



The system log tracks the important events and setting changes of the AP. If the AP is rebooted, the logs are automatically cleared.

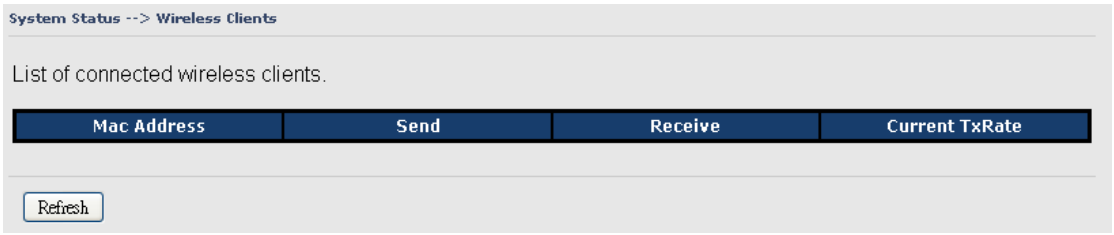
Click the button '**Refresh**' to refresh the page; Click the button '**Clear**' to clear log entries.

Traffic Statistics



This page displays the network traffic statistics for both received and transmitted packets through the Ethernet port and wireless connections associated with the AP. Simultaneity, the traffic counter will reset by the device rebooting.

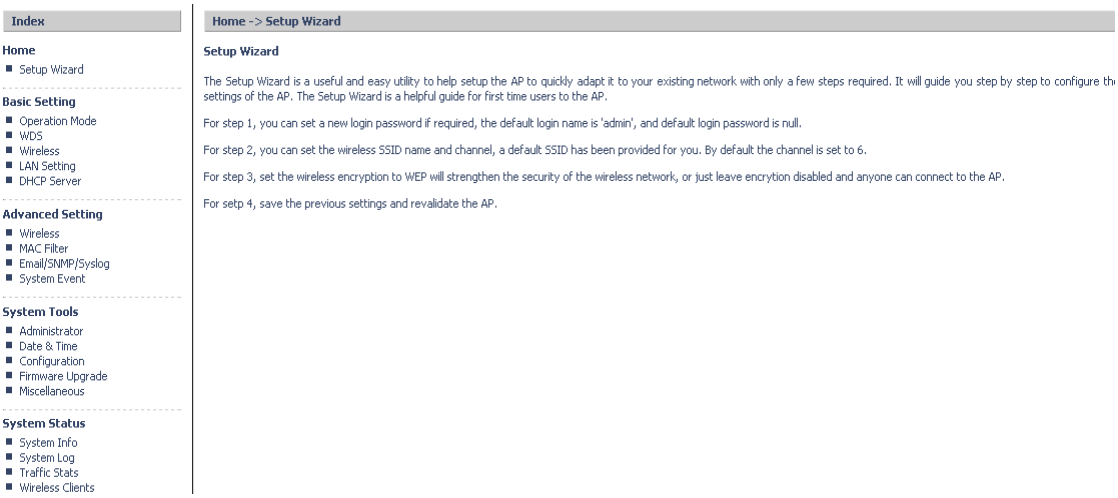
Wireless Clients



This page of the list displays the **Mac Address** of the wireless clients connected. **Current TX Rate** is corresponding to the **Transmission Rate** in the **Advanced Setting > Wireless** pages.

5.5.5 Online Help

Click on any item in the **Online Help** screen for more information.


Index
Home
Setup Wizard
Basic Setting
Operation Mode
WDS
Wireless
LAN Setting
DHCP Server
Advanced Setting
Wireless
MAC Filter
Email/SNMP/Syslog
System Event
System Tools
Administrator
Date & Time
Configuration
Firmware Upgrade
Miscellaneous
System Status
System Info
System Log
Traffic Stats
Wireless Clients
Home -> Setup Wizard
Setup Wizard
The Setup Wizard is a useful and easy utility to help setup the AP to quickly adapt it to your existing network with only a few steps required. It will guide you step by step to configure th
settings of the AP. The Setup Wizard is a helpful guide for first time users to the AP.
For step 1, you can set a new login password if required, the default login name is 'admin', and default login password is null.
For step 2, you can set the wireless SSID name and channel, a default SSID has been provided for you. By default the channel is set to 6.
For step 3, set the wireless encryption to WEP will strengthen the security of the wireless network, or just leave encrytion disabled and anyone can connect to the AP.
For setp 4, save the previous settings and revalidate the AP.

Technical Specifications

LAN Interface	
RJ45 Ports	1 x 10/100Base-T(X), Auto MDI/MDI-X
Protocols	IP, TCP, UDP, DHCP, BOOTP, ARP/RARP, DNS, SNMP MIB II, HTTPS, SNMPV1/V2, Trap, Private MIB
WLAN Interface	
Operating Mode	AP/Bridge/Repeater/AP-Client/Client
Antenna Connector	2 x External N-type antenna connector for IAP-W512+, Build-in 15dBi panel antenna for IAP-W510+
Radio Frequency Type	OFDM
Modulation	IEEE802.11a : OFDM with BPSK, QPSK, QAM, 64QAM IEEE802.11n : BPSK, QPSK, 16-QAM, 64-QAM
Frequency Band	America / FCC : 5.180 to 5.825 GHz (9 channels) Europe CE / ETSI : 5.180 to 5.240 GHz (4 channels)
Transmission Rate	IEEE802.11a: 6/ 9/ 12/ 18/ 24/ 36/ 48/ 54 Mbps IEEE802.11n: up to 300Mbps
Transmit Power	IEEE802.11a/n: 500mw
Receiver Sensitivity	-82dBm @ 54Mbps, PER< 10%; -78dBm@MCS 15(11n, 20MHz), PER< 10%; -75dBm@MCS 15(11n, 40MHz), PER< 10%
Encryption Security	WEP: (64-bit ,128-bit key supported) WPA/WPA2 :802.11i(WEP and AES encryption) WPAPSK (256-bit key pre-shared key supported)
Wireless Security	SSID broadcast disable
LED Indicators	1. PWR: 1 x LED Green On: Power is on and functioning Normally.

	2. LAN: 1 x LED Green On: Port Link Green Blinking: Transmitting data 3. WLAN: 1 x LED Green for WLAN Link/ Act
Power Requirements	
Power Input Voltage	Fully Compliant with IEEE802.3af
Power Consumption	9 Watts
Environmental	
Operating Temperature	-20 to 70°C
Storage Temperature	-30 to 85°C
Operating Humidity	100% non-condensing
Mechanical	
Dimensions(W x D x H)	162 mm(W)x 102 mm(D)x 58 mm(H) for IAP-W510 162 mm(W)x 102 mm(D)x 48 mm(H) for IAP-W512
Casing	IP-67 protection
Regulatory Approvals	
Regulatory Approvals	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC 60068-2-27
Free Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6
Safety	EN60950-1
Warranty	3 years